IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

IN RE CROWDSTRIKE HOLDINGS, INC. SECURITIES LITIGATION	Civil Action No. 1:24-cv-00857-RP

DEFENDANTS' MOTION TO DISMISS PLAINTIFF'S CONSOLIDATED CLASS ACTION COMPLAINT

Sandra C. Goldstein, P.C. (*pro hac vice*)
Kevin M. Neylan, Jr. (*pro hac vice*)
KIRKLAND & ELLIS LLP
601 Lexington Avenue
New York, NY 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900
Email: sandra.goldstein@kirkland.com
kevin.neylan@kirkland.com

Steven J. Wingard (State Bar No. 00788694)
Santosh Aravind (State Bar No. 24095052)
Robert "Robby" Earle (State Bar No. 24124566)
SCOTT DOUGLASS & McCONNICO LLP
303 Colorado Street, Suite 2400
Austin, TX 78701
Telephone: (512) 495-6300
Facsimile: (512) 495-6399
Email: swingard@scottdoug.com
saravind@scottdoug.com
rearle@scottdoug.com

Counsel for Defendants

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Heck v. Orion Grp. Holdings, Inc.,
468 F. Supp. 3d 828 (S.D. Tex. 2020) .... *passim*

Inclusive Cmtys. Project, Inc. v. Lincoln Prop. Co.,
920 F.3d 890 (5th Cir. 2019) 4, 8

Ind. Elec. Workers' Pension Tr. Fund IBEW v. Shaw Grp. Inc.,
537 F.3d 527 (5th Cir. 2008) 8, 32, 34

Izadjoo v. Helix Energy Sols. Grp., Inc.,
237 F. Supp. 3d 492 (S.D. Tex. 2017) .... *passim*

Johnson v. Callanen,
610 F. Supp. 3d 907 (W.D. Tex. 2022)..........22

KB Partners I, L.P. v. Pain Therapeutics, Inc.,
2012 WL 12850252 (W.D. Tex. Sept. 26, 2012)..........21

In re Key Energy Servs., Inc. Sec. Litig.,
166 F. Supp. 3d 822 (S.D. Tex. 2016) 9, 29, 33

Linenweber v. Southwest Airlines Co.,
693 F. Supp. 3d 661 (N.D. Tex. 2023) .... *passim*

Loc. 731 I.B. of T. Excavators & Pavers Pension Tr. Fund v. Diodes, Inc.,
67 F. Supp. 3d 782 (E.D. Tex. 2014), *aff'd*, 810 F.3d 951 (5th Cir. 2016) 11, 12

Loc. 731 I.B. of T. Excavators & Pavers Pension Tr. Fund v. Diodes, Inc.,
810 F.3d 951 (5th Cir. 2016) 21

Macquarie Infrastructure Corp. v. Moab Partners, L.P.,
601 U.S. 257 (2024)..........25

MicroCapital Fund LP v. Conn's Inc.,
2019 WL 3451153 (S.D. Tex. July 24, 2019)..........3

Neiman v. Bulmahn,
854 F.3d 741 (5th Cir. 2017) 29

Ohio Pub. Emps. Ret. Sys. v. Meta Platforms, Inc.,
2024 WL 4353049 (N.D. Cal. Sept. 30, 2024) 20

Owens v. Jastrow,
789 F.3d 529 (5th Cir. 2015) .... *passim*

Sask. Healthcare Emp.'s Pension Plan v. KE Holdings Inc.,
718 F. Supp. 3d 344 (S.D.N.Y. 2024)..........13

Statutes

Rules

Defendants respectfully submit this motion to dismiss and brief in support. Pursuant to the PSLRA and Rules 8, 9(b), and 12(b)(6), the Complaint should be dismissed with prejudice.

INTRODUCTION

CrowdStrike's July 19, 2024 incident was an unfortunate event, but it did not reveal any securities fraud. The first essential element of any securities fraud case is a false or misleading statement. But here, plaintiff fails to allege any actionable false or misleading statements. Instead, plaintiff's case rests on a foundation of egregious distortions of CrowdStrike's public statements, with plaintiff repeatedly ripping those statements out of context to build its purported fraud case. For example, plaintiff alleges that CrowdStrike misled investors about a quality assurance team dedicated *to testing software updates*—but the statements plaintiff points to, when considered in their true context, are about CrowdStrike's quality assurance team dedicated to making its products *accessible to the visually impaired*. Similarly, plaintiff alleges that CrowdStrike misrepresented the process it followed when updating *its own* software—but the statements plaintiff points to are actually CrowdStrike explaining how one of its products helps *customers* secure *their* software, and say nothing whatsoever about CrowdStrike's *own* software development process. A securities case premised on allegations that are contextual distortions cannot proceed.

As far as plaintiff's theory of falsity is concerned, it fails based on these contextual distortions alone. In addition, plaintiff's theory of falsity fails independently because it is premised on the assertion that the July 19 incident occurred because CrowdStrike released a *software* update, and therefore revealed alleged misstatements about CrowdStrike's process for releasing software updates. However, the very documents cited and incorporated into the Complaint make clear that the incident was not triggered by the release of a software update at all, but rather by a very different kind of update, a *content* update, which is a transmission of data and not software at all. As a result, the incident revealed nothing about CrowdStrike's process for releasing software updates. When this mischaracterization is corrected, which it must be as a matter of law, plaintiff's case collapses like a house of cards.

The Complaint's factual allegations that are attributed to former employee confidential witnesses cannot rectify plaintiff's case. The confidential witnesses are not even alleged to have occupied positions at CrowdStrike that would have given them access to the information attributed to them. None of these former employees are alleged to have worked directly on software updates or content updates, none are alleged to have had direct contact with CrowdStrike executives, and only one even allegedly worked at CrowdStrike during the July 19 incident. These allegations are all but worthless and should not be credited. Moreover, plaintiff's theory of falsity is contradicted by CrowdStrike's disclosures to investors and amounts to a legally impermissible claim of fraud by hindsight. For all these reasons, the falsity allegations fail and the claims must be dismissed.

The second essential element of any securities fraud case is sufficient allegations of scienter, giving rise to a strong inference that defendants made the alleged misstatements with an intent to deceive, manipulate, or defraud, or were severely reckless. Yet, strikingly absent from the Complaint is any theory of motive on the part of any defendant, including CrowdStrike's CEO George Kurtz, and its President Michael Sentonas, who are not alleged to have benefited in any personal or particular way from their alleged fraud. All plaintiff alleges is that Kurtz and Sentonas acted with the same motive as every corporate executive in the country—to maximize profits and shareholder value. And so far as plaintiff alleges, Kurtz and Sentonas were harmed right alongside CrowdStrike's other shareholders when its stock price dropped after the incident. Without any theory of motive, plaintiff's burden to plead scienter is that much more difficult to sustain. Plaintiff cannot do so. The Complaint essentially alleges that Kurtz and Sentonas knowingly and deliberately set CrowdStrike on a path to inevitable catastrophe, by having CrowdStrike ignore software testing features that everyone, including Kurtz and Sentonas, supposedly knew were essential to avoiding events like the July 19 incident. That story is incoherent, and nothing in the Complaint comes close to creating a strong inference that it is true. This hole in plaintiff's theory also independently requires dismissal.

BACKGROUND

For purposes of this motion only, CrowdStrike assumes the truth of well-pled allegations in the Complaint, except when they contradict facts that are subject to judicial notice or are incorporated by reference in the Complaint. *See, e.g.*, *In re Plains All Am. Pipeline, L.P. Sec. Litig.*, 307 F. Supp. 3d 583, 598 (S.D. Tex. 2018). The Court may take judicial notice of SEC filings and earnings call transcripts. *MicroCapital Fund LP v. Conn's Inc.*, 2019 WL 3451153, at *4 n.6 (S.D. Tex. July 24, 2019). And the alleged misstatements must be considered in their full context, as a reasonable investor would have understood them. *See, e.g.*, *Linenweber v. Southwest Airlines Co.*, 693 F. Supp. 3d 661, 680 (N.D. Tex. 2023) (dismissing complaint where "[p]laintiffs charge [d]efendants with two misstatements that are neither false nor misleading when considered in the context from which [p]laintiffs removed them").

A. The Falcon Platform and the July 19 Incident

CrowdStrike was founded in 2011 and is a leader in cybersecurity. One way that CrowdStrike protects its customers is through the Falcon platform. (¶¶20-23.)[1] The Falcon platform uses a combination of cloud and on-device security to deliver real-time threat detection and response. (¶21.) CrowdStrike customers install a small piece of software called the Falcon sensor on endpoints, such as laptops, desktops, and servers. *Id.* The Falcon sensor and

[1] References to "¶" are to the Consolidated Class Action Complaint (the "Complaint" for short). All emphases in quotations have been omitted unless otherwise noted.

CrowdStrike's security cloud are in regular communication with each other to help protect against emerging threats, such as ransomware and data breaches. (¶¶21-23.)

To ensure that CrowdStrike customers have the latest protection, the Falcon sensor receives threat detection content updates called Rapid Response Content updates, among other updates. (*Id.*) Rapid Response Content is not software or code—rather, it is configuration data that the Falcon sensor uses to look for and protect against new cybersecurity threats. (Ex. A, at 1, 8.)[2] To use a simplified analogy, the Falcon sensor is like a security guard looking for threats, and Rapid Response Content updates are like security briefings, updated with the latest instructions to look for threats according to currently available information.

On July 19, 2024, CrowdStrike released two Rapid Response Content updates, which were directed to address a new cyber threat. One of these Rapid Response Content updates triggered an error, which unexpectedly led to a blue-screen system crash on some computers that were online from 12:09 AM EDT to 1:27 AM EDT running Microsoft Windows. (¶¶9, 77.) The issue that caused the outage had evaded multiple layers of CrowdStrike's validation and testing. (Ex. A, at 2.) There had never been a significant problem caused by a Rapid Response Content update before the July 19 incident, and plaintiff does not allege otherwise.

A recurring theme of the Complaint is that the July 19 incident was triggered when CrowdStrike released a software update, and thus revealed that CrowdStrike's process for deploying software updates was deficient. (*E.g.*, ¶1.) But that allegation ignores that Rapid Response Content is not software or code, and Rapid Response Content updates do not involve

[2] Exhibits employ yellow highlighting to identify passages referred to in this brief or the appendix, and blue highlighting to identify passages quoted in the Complaint. These exhibits are properly before the Court because they are each subject to judicial notice, are incorporated by reference in the Complaint, or both. *Plains All Am.*, 307 F. Supp. 3d at 598; *Inclusive Cmtys. Project, Inc. v. Lincoln Prop. Co.*, 920 F.3d 890, 900 (5th Cir. 2019).

changing the software or code in the Falcon sensor. (Ex. A, at 1, 8; Ex. B, at 2.) In other words, transmitting a Rapid Response Content update does not involve developing new software or code, or rolling out software or code changes. As a result, the outage did not reveal *anything* about CrowdStrike's processes for transmitting software or code updates to customers.[3]

B. The Alleged Misstatements

Looking for any possible hook to transform the July 19 incident into a case of securities fraud, plaintiff has resorted to mischaracterizing CrowdStrike's public statements beyond recognition. Plaintiff alleges that between September 20, 2022, and July 30, 2024, Defendants made fifteen actionable misstatements. (¶¶120-46.) The alleged misstatements are set forth below, and are reproduced in full in the accompanying Appendix A. Plaintiff claims that each challenged statement was materially false or misleading for four reasons: because CrowdStrike supposedly (1) did not "test[] its software updates in a pre-production environment," (2) did not "release[] its software updates through an industry-standard, phased rollout," (3) did not "ha[ve] a dedicated quality assurance team" for software updates, and (4) did not "follow[] the requirements of" the Federal Risk and Authorization Management Program ("FedRAMP") and the Department of Defense ("DoD"). (¶118.) None of those factual allegations even *could* render the challenged statements false or misleading, and plaintiff's attempt to allege otherwise requires divorcing the

[3] Rapid Response Content updates are subject to rigorous testing, including validation checks and stress tests before deployment. (Ex. B, at 2.) But because Rapid Response Content updates are not code or software, the time-consuming process for testing software updates is not appropriate for them, as all reasonable investors would have understood based on CrowdStrike's public disclosures. CrowdStrike disclosed that planning, developing, and testing software updates takes "a significant amount of time." (Ex. C, at 35.) And, as plaintiff acknowledges, CrowdStrike also disclosed that Rapid Response Content updates work best if they are deployed quickly based on the latest threat intelligence. (¶¶22-23.) As such, no reasonable investor would have expected Rapid Response Content updates to be subjected to the same time-consuming process for testing software updates before they could be released.

challenged statements from their context and attributing meanings to them that no reasonable investor would have understood.

The alleged misstatements fall into four categories:

1. Accessibility Statements. The first category includes two statements that relate to testing whether CrowdStrike's customer-facing user interfaces (which are web-based) are visually accessible to people with impaired vision. The two statements describe how CrowdStrike maintains a "quality assurance team" that assists with "testing for accessibility." (¶136.) As explained below, when read in context, these statements told investors that CrowdStrike strives to make sure visually impaired people can use the interface on its products. Contrary to plaintiff's distortions, these statements say nothing about how CrowdStrike tests software updates, how it releases software updates, how it performs quality assurance on software updates, or its compliance with FedRAMP and DoD regulations. Plaintiff's factual allegations on those subjects therefore cannot render the Accessibility Testing Statements false or misleading.

2. Product Usage Statements. The second category includes six statements about how CrowdStrike's *customers* can use the Falcon platform to keep their own code secure and to perform other tasks on their own computer networks. (¶¶124, 126, 128, 130, 132, 145.) In context, these statements say nothing about how *CrowdStrike* tests software updates, releases software updates, performs quality assurance on software updates, or complies with FedRAMP and DoD regulations. Plaintiff's factual allegations on those subjects therefore cannot render the Product Usage Statements false or misleading.

3. Software and Testing Statements. The third category includes statements related to software and/or testing, but *not* testing of *content* updates. (¶¶120, 122, 134, 139.) These statements cannot support a claim of securities fraud for several reasons, including that plaintiff

takes them out of context, targets non-actionable puffery, and challenges statements that are not alleged to have been false when made. In addition, as explained, the July 19 incident was triggered by the release of a *content* update, not a software update, and therefore did not reveal anything about CrowdStrike's process for releasing software updates. Although not necessary to defeat plaintiff's theory of falsity with respect to the Software and Testing statements, this circumstance means that those statements are not rendered false or misleading by plaintiff's factual allegations.

4. Regulatory Compliance Statements. Finally, plaintiff targets two statements that affirm that CrowdStrike met FedRAMP and DoD regulatory requirements. (¶¶141, 143.) These allegations fail. The Court can take judicial notice of the fact that, according to the federal government's own website, CrowdStrike *is* authorized by both FedRAMP and DoD. (Ex. D, at 68; Ex. E, at 5.) Plaintiff cannot contest the truth of that fact. Furthermore, as a matter of law, plaintiff misrepresents the contents of the relevant FedRAMP and DoD requirements, which do not line up with plaintiff's allegations. Plaintiff therefore cannot rely on the Regulatory Compliance Statements to support a claim of securities fraud.

ARGUMENT

I. PLAINTIFF'S SECTION 10(B) CLAIM SHOULD BE DISMISSED.

To successfully plead a Section 10(b) claim, plaintiff must properly allege: "(1) a material misrepresentation (or omission), (2) scienter, *i.e.*, a wrongful state of mind, (3) a connection with the purchase or sale of a security, (4) reliance …; (5) economic loss; and (6) loss causation." *Owens v. Jastrow*, 789 F.3d 529, 535 (5th Cir. 2015). "If a complaint fails to meet the pleading requirements of the PSLRA or Rule 9(b), the complaint must be dismissed." *ABC Arbitrage Pls. Grp. v. Tchuruk*, 291 F.3d 336, 350 (5th Cir. 2002).

A. Plaintiff Fails to Plead Any Actionable Misstatements or Omissions

At this stage of the case, although well-pled allegations are generally assumed true, plaintiff is not entitled to a presumption that it has accurately characterized the statements alleged to be false or misleading—a principle that is dispositive here, because, as detailed below, the Complaint rests on pervasive, rampant mischaracterizations of Defendants' statements that take them out of context and distort them beyond recognition. *See, e.g.*, *Linenweber*, 693 F. Supp. 3d at 680. In addition, as noted above, allegations will not be assumed true if they contradict facts that are subject to judicial notice or are incorporated by reference. *See, e.g.*, *Plains All Am.*, 307 F. Supp. 3d at 598. The Complaint contains many allegations that are not entitled to an assumption of truth for this reason as well, including plaintiff's refrain that the July 19, 2024 incident was triggered by the release of a *software* update. That assertion is contradicted by the Post Incident Review and Root Cause Analysis, which the Complaint cites numerous times. (¶¶69, 91-92, 163-64.) The Court may consider these documents now. *E.g.*, *Inclusive Cmtys. Project, Inc.*, 920 F.3d at 900 ("When a defendant attaches documents to its motion that are referenced in the complaint and are central to the plaintiff's claims, … the court can also properly consider those documents."). Furthermore, the Court may take judicial notice of SEC filings and earnings call transcripts, *Firefighters Pension & Relief Fund of the City of New Orleans v. Bulmahn*, 53 F. Supp. 3d 882, 902 (E.D. La. 2014), which here demonstrate that plaintiff has repeatedly taken Defendants' statements out of context.

In addition, factual allegations attributed to former employee confidential witnesses ("FEs") must be severely discounted when—as here—the facts as pled do not show that there is a high probability that the FEs would possess relevant information by virtue of their position at the company. *In re Dell Inc., Sec. Litig.*, 591 F. Supp. 2d 877, 895-96 (W.D. Tex. 2008); *Ind. Elec. Workers' Pension Tr. Fund IBEW v. Shaw Grp. Inc.*, 537 F.3d 527, 535 (5th Cir. 2008) ("courts must discount allegations from confidential sources"). Here, *none* of the eight FEs are alleged to have worked directly on sensor code or content updates, *none* of the FEs alleges that they had direct contact with CrowdStrike executives, and only *one* FE (FE-2) even allegedly worked at CrowdStrike during the July 19 incident. When properly discounted as required under Fifth Circuit precedent, plaintiff's FE-based allegations are rendered nearly worthless. *E.g.*, *In re Key Energy Servs., Inc. Sec. Litig.*, 166 F. Supp. 3d 822, 862 (S.D. Tex. 2016) (rejecting confidential witness allegations because "[t]here [were] no allegations that three of the four Individual Defendants … had any communications with the CW[s]"). Finally, for plaintiff to meet the heightened pleading standard for securities fraud, it must plead falsity with specificity, not only setting forth with particularity "the time, place, the identity of the speaker, and the content of the alleged misrepresentation," but also explaining why each alleged misstatement is misleading. *Southland Sec. Corp. v. INSpire Ins. Sols. Inc.*, 365 F.3d 353, 362 (5th Cir. 2004); 15 U.S.C. § 78u-4(b)(1)(B). As demonstrated below, this lawsuit is built on a foundation—the fifteen alleged misstatements—that crumbles under scrutiny, because it depends on taking those statements out of context and reading them in ways no reasonable investor would have understood them.

1. The Accessibility Statements Are Not Properly Alleged to be False.

Starting with the Accessibility Statements, plaintiff strips them of their context, fails to allege facts contradicting the statements, and improperly relies on deficient FE allegations.

Plaintiff repeatedly alleges CrowdStrike concealed that it did not have a "quality assurance team" to test software. (*See, e.g.*, ¶¶5, 9, 33, 50, 59, 137.) This entire theory of falsity rests on alleged misstatements in CrowdStrike's 2023 and 2024 Proxy Statements that CrowdStrike's "quality assurance team … test[s] for accessibility." (¶136.) The statements, however, refer *solely* to CrowdStrike testing its products for accessibility for the visually impaired—they have nothing at all to do with the testing of software or content updates. Even a cursory reading of the relevant statements show that they appear under a heading entitled "Accessibility," and say, in full that:

> *CrowdStrike takes accessibility of its products very seriously*, with dedicated accessibility specialists on staff as part of a program of continuous education on accessible design and engineering for those working on our customer-facing user-interfaces. In particular, we focus on screen reader compatibility for visually impaired users and color/contrast configurability to optimize our experience for various classes of color-blindness. *Our quality assurance team is also trained and equipped to assist with testing for accessibility* and we work with external accessibility auditors to help identify any deficiencies.

(Ex. F, at 18 (emphasis added); *see also* Ex. G, at 18 (similar).)

Here, plaintiff strips the Accessibility Statements from their context and flagrantly mischaracterizes them. Despite plaintiff's contention that the Accessibility Statements refer to software testing, (¶137), the statements—as just shown—plainly refer to testing the "accessibility of [CrowdStrike's] products for ***differently abled users***" and make no mention of CrowdStrike's software or content updates. (Ex. F, at 18; Ex. G, at 18 (emphasis added).) The Accessibility Statements are therefore not properly alleged to be false, because a proper falsity allegation would require plaintiff to plead particularized facts showing that CrowdStrike did not have a quality assurance team that tested its products for accessibility to differently abled users. But falsity cannot be pled by stripping a statement of its context. *Linenweber*, 693 F. Supp. 3d at 680.

Moreover, plaintiff's only claimed factual support for its allegation that CrowdStrike had no quality assurance team for software comes from the FEs. Even if fully credited, these FE-based allegations do not falsify the Accessibility Statements, for the simple reason that the FEs do not allege that CrowdStrike lacked a quality assurance team for *accessibility*, as they must to contradict the Accessibility Statements. *See Linenweber*, 693 F. Supp. 3d at 680-81 (finding that plaintiff failed to plead falsity when failing to allege contradictory facts after statement was considered in full context). Plaintiff does not make any such allegation, which is not surprising because quality assurance for accessibility has nothing to do with the July 19 incident.

In addition, plaintiff's FE-based allegations are not entitled to meaningful weight and thus cannot prop up plaintiff's allegations. Courts in the Fifth Circuit "*must* discount allegations from confidential sources," even at the motion-to-dismiss stage—the only question is the "degree" of the discount. *Genesee Cnty. Emps.' Ret. Sys. v. FirstCash Holdings Inc.*, 667 F. Supp. 3d 295, 306-07 (N.D. Tex. 2023). This is because "[u]nder the PSLRA's heightened pleading standard, the process for weighing inferences is obstructed when the witness is anonymous." *Id.* at 306. Therefore, before FEs can be credited, plaintiff must describe them with "sufficient particularity to support the probability that a person in the position occupied by the source as described would possess the information pleaded to support the allegations of false or misleading statements." *Izadjoo v. Helix Energy Sols. Grp., Inc.*, 237 F. Supp. 3d 492, 510 (S.D. Tex. 2017).

Here, plaintiff relies on the allegations of FE-1, FE-3, FE-4, and FE-5, all of whom allege that CrowdStrike did not have a dedicated quality assurance team for software testing. (*See* ¶70-76.) Putting aside that these allegations do not falsify any statements alleged in the Complaint, even if they did, the FE allegations would still fail for lack of specificity and reliability. *None* of those FEs is alleged to have worked on quality assurance, and thus none are in a position to speak to CrowdStrike's company-wide quality assurance policies. *Loc. 731 I.B. of T. Excavators & Pavers Pension Tr. Fund v. Diodes, Inc.*, 67 F. Supp. 3d 782, 788 (E.D. Tex. 2014), *aff'd*, 810 F.3d 951 (5th Cir. 2016) ("*Diodes I*") (rejecting FE allegations where plaintiff failed to allege that certain responsibilities were within FE's job description). For example, FE-1 was allegedly "a Senior Technical Operations Engineer on the forensics team," and was allegedly "responsible for testing of the forensic system for Falcon." (¶62 n.67.) Plaintiff does not explain what that role involved, and notably does not allege that it related to quality assurance. CrowdStrike's website reveals that the forensics team's work related to "data collection" and "analysis of cybersecurity incidents." (Ex. H, at 1.) In other words, FE-1's position had nothing to do with quality assurance, content updates, coding, or software development or testing, and plaintiff does not allege otherwise. Similarly, FE-3 was allegedly a "Software Engineer," FE-4 was allegedly "Director of Engineering for infrastructure," and FE-5 was allegedly "a Provisioning Engineer," but plaintiff offers no detailed, particularized allegations that *any* of these roles involved quality assurance, content updates, coding, or software development or testing. (*See* ¶67 n.71, ¶70 nn.78-79.)

Furthermore, every one of these FEs left CrowdStrike before the July 19 incident—and three of the four (FEs 1, 3, and 4) left between September 2022 and October 2023, or nine months to nearly two years before the July 19 incident. (¶62 n.67, ¶67 n.71, ¶70 nn.78-79.) Given that none of these FEs worked in the relevant area of CrowdStrike, and that they all left well before the July 19 incident, their allegations must be discounted entirely or, at the very least, steeply. *See Diodes I*, 67 F. Supp 3d at 788; *Dell*, 591 F. Supp. 2d at 895. These deficient FE allegations do not remedy plaintiff's failure to plead falsity of the Accessibility Statements.

2. The Product Usage Statements Are Not Properly Alleged to be False.

Plaintiff alleges the Product Usage Statements—six statements in which CrowdStrike described various ways that customers use its product—were false and misleading. (¶¶124, 126, 128, 130, 132, 145.) But like the Accessibility Statements, plaintiff significantly mischaracterizes the Product Usage Statements. Even a cursory read of the surrounding context—which the Complaint omits entirely, but the Court may and should consider in assessing the adequacy of the pleadings—reveals that none of the statements mention CrowdStrike's own testing or quality control at all. *See Linenweber*, 693 F. Supp. 3d at 680 (statements must be read in context).

First, plaintiff challenges a statement in an article on CrowdStrike's website about the "continuous integration and continuous delivery (CI/CD)" pipeline. (¶145.) Plaintiff alleges that CrowdStrike "stated [in the article] that it [*i.e.*, CrowdStrike] deployed software updates to a '***staging environment that closely resembles the production environment***,'" but the article makes no such claim. (*Id.*) The article is part of CrowdStrike's "Cybersecurity 101" educational series, which explains how threat actors target customers' CI/CD pipelines. (Ex. I, at 1, 3.) Critically, the article says nothing whatsoever about CrowdStrike's own process for updating software or Rapid Response Content, and it makes no representation that CrowdStrike employs CI/CD at all. Instead, the article describes CrowdStrike as "a trusted security partner in *your* [*i.e.*, *the customer's*] corner" to "protect[] *your* pipeline" while customers update *their own* software, and notes that "deploy[ing]" software updates "to a staging environment that closely resembles the production environment" is part of a "*typical [CI/CD] task flow*." (*Id.* at 2, 3 (emphasis added).)

There is no factual allegation in the Complaint that renders the CI/CD article false or misleading. The Complaint does not allege that the July 19 incident was in any way related to the CI/CD software development process—let alone the CI/CD development process of CrowdStrike's customers. Moreover, because the article in no way states or implies that CrowdStrike tested software or Rapid Response Content updates in staging environments, plaintiff's allegation that CrowdStrike did *not* do so cannot render the CI/CD article false or misleading. The CI/CD article therefore cannot support a claim of securities fraud. *See Linenweber*, 693 F. Supp. 3d at 680-81; *see also Sask. Healthcare Emp.'s Pension Plan v. KE Holdings Inc.*, 718 F. Supp. 3d 344, 377 (S.D.N.Y. 2024) ("[P]laintiffs may not cherry pick certain public statements … and divorce them from the universe of disclosed information.").

Second and third, plaintiff targets two statements by Kurtz: one where he stated that one of Falcon's "capabilities" is that it can "understand if insecure code is being put into the CI/CD pipeline," and a second where he stated that "Falcon Cloud Security" has the "ability to help make sure that code is secure, that it's deployed and that it's run in a secure environment." (¶¶124, 126.)

Plaintiff alleges these statements are false or misleading because CrowdStrike allegedly did not test its own software to "make sure that *its* [*i.e.*, *CrowdStrike's*] code is secure." (¶127 (emphasis added); *see* ¶125 (similar).) But as with the CI/CD article described above, plaintiff omits context that makes clear these statements by Kurtz are about how Falcon can protect customers *when customers update their own [i.e., non-CrowdStrike] product's code*—not what happens when *CrowdStrike* updates *CrowdStrike's* code. For example, after saying that one of Falcon's "capabilities" was helping "understand if insecure code is being put into the CI/CD pipeline," Kurtz explained that this feature was important because "customers" were "moving to our solution" and were "seeing the benefits of an integrated platform with Falcon." (Ex. J, at 15.) Similarly, when Kurtz stated that the "Falcon Cloud Security" has the "ability to help make sure that code is secure, that it's deployed and that it's run in a secure environment," he was describing "CSPM [*i.e.*, Cloud Security Posture Management] and Cloud Workload Protection," (Ex. K, at 11), which CrowdStrike explained are services CrowdStrike offers to "provide[] visibility into *your* [*i.e.*, *customers'*] cloud security," (Ex. L, at 1 (emphasis added)), and to "offer[] unified cloud workload protection across multiple providers," (Ex. M, at 1). In context, it is plain that Kurtz's statements are about how customers use Falcon Cloud Security to secure their cloud environments, and do not represent anything about the process CrowdStrike followed when updating *sensor* code or rolling out *Rapid Response Content* updates. Plaintiff's factual allegations therefore once again do not and cannot render what Defendants actually said false or misleading.

Fourth and fifth, plaintiff mischaracterizes two statements about a CrowdStrike product called Falcon for IT, alleging that it was false or misleading for CrowdStrike to "state that customers 'can use Falcon for IT' to avoid 'blue screens,'" (¶129 (citing Ex. N, at 15)), and "that CrowdStrike's Falcon software 'fix[es]' technology to avoid 'blue screens'" (¶131 (citing Ex. O, at 17-18)). For example, plaintiff points to a comment by Kurtz that "[w]e've got many, many airlines that use our technology. They don't want to send out an IT person to go fix a kiosk that has a Microsoft blue screen. So what can they do? They can use Falcon for IT." (¶128.) Keying in on the phrase "blue screen," plaintiff asserts that Kurtz was "assur[ing] analysts and investors that CrowdStrike's Falcon software updates avoid 'blue screen' errors," (¶128), but that is an egregious distortion. The full context immediately makes clear that Kurtz's comment did not say a word about CrowdStrike's software updates, let alone the risk that software updates would cause blue screen errors. Kurtz was explaining that when customers have IT problems, they can use Falcon for IT to generate "tremendous savings in terms of cost and travel and complexity," because Falcon for IT has "automation" capabilities that can be used to "bring [customers' systems] back to health" automatically and remotely. (Ex. N, at 15.) As CrowdStrike disclosed, Falcon for IT is used by customers to scan their networks to detect endpoints (*i.e.*, computers) that are experiencing blue-screen errors and then to remotely reboot them. (*See* Ex. C, at 11; *see also* Ex. AA, at 9.) Kurtz's statements once again say nothing whatsoever about the process CrowdStrike followed for testing software or Rapid Response Content updates, or about the risks of blue screen errors from such updates. And there is no allegation that CrowdStrike's customers *did not* use Falcon for IT to remotely reboot endpoints, which is all that Kurtz actually said in these statements. Nor is there is any allegation that Falcon for IT had anything to do with what caused the July 19 incident. When read in context, these two statements are not properly alleged to be false.

Sixth, plaintiff alleges that Sanjay Chaudhary, VP of Product Management, made a false statement on April 18, 2024, when he said CrowdStrike customers can use CrowdStrike's application programming interface ("API") to "build" custom "detections" themselves, which they can then "test [] in non-production environments" before "roll[ing] them out" themselves. (¶132.)

Plaintiff misinterprets the statement as CrowdStrike "stat[ing] that it tests its updates 'in non-production environments,'" but the statement says nothing about CrowdStrike's *own* testing. (¶133.) Chaudhary was referring to customers building their own updates and deploying those updates themselves, to their own systems, using Falcon's API, which is a tool that helps software developers build their own solutions. (¶132 (quoting Ex. P, at 11) ("[O]ur focus has always been an API-first and foremost. We don't want *you* to just to go on the UI and build one detection. Rather, programmatically build hundreds of detections, test those in non-production environments, and roll them out." (emphasis added)).) Again, the true context refutes plaintiff's falsity allegation.

Despite none of the six Product Usage Statements saying anything about CrowdStrike's own testing or updates, plaintiff relies heavily on them throughout the Complaint, attempting to cobble them and other inapposite statements together to allege falsity. (*E.g.*, ¶¶4, 23, 35, 46-48.) These strained efforts are not persuasive. The lengths to which plaintiff has gone to attempt to manufacture a false statement all but prove that the July 19 incident did not reveal securities fraud.

3. The Software and Testing Statements Are Not Properly Alleged to be False.

Plaintiff alleges that the Software and Testing Statements—five generalized statements about CrowdStrike's testing and/or software updates—are false or misleading. (¶¶120, 122, 134, 139.) These allegations fare no better than the allegations about the statements discussed above.

As a threshold matter, plaintiffs repeatedly and incorrectly conflate *software* or *code* testing with Rapid Response Content testing, when these two items and processes are different. (Ex. A, at 1, 8; Ex. B, at 2.) Plaintiff completely ignores this distinction and claims that CrowdStrike "led [] investors to believe that [it] adhered to [] basic, industry-standard requirements before releasing [its] Falcon ***software*** updates," while concealing that it did not. (¶2 (emphasis added).) Plaintiff alleges that CrowdStrike concealed that it "did not test [its] ***software*** updates in a pre-production environment," that it "released [its] ***software*** updates to all customers at the same time," and that it "lacked a dedicated quality assurance team … and test[ing] plans for [its] ***software*** updates." (¶119 (emphases added).) Plaintiff fails to even acknowledge that Rapid Response Content updates are not software updates, as Rapid Response Content is not software or code, (Ex. A, at 1, 8; Ex. B, at 2)—and plaintiff points to no statement in which CrowdStrike ever said Rapid Response Content updates *are* software or code. Plaintiff even misrepresents the sworn Congressional testimony of CrowdStrike executive Adam Meyers. Plaintiff asserts that "Mr. Meyers confirmed that CrowdStrike did ***not*** test software updates in a pre-production environment prior to release to the public and did ***not*** conduct phased rollouts of its software updates." (¶94; *see also* ¶¶66, 68.) But Meyers said the exact *opposite*. Meyers testified—in response to a question that characterized the update as a "software update"—that "the content update was not code." (Ex. Q, at 18.) Moreover, plaintiff ignores that Meyers repeatedly explained that content updates are not software or code, that CrowdStrike *did* test its actual software and code in pre-production environments and then released it in phased rollouts, and that content updates were subject to different—but still thorough—testing before the July 19 incident, because they are not code. (*See id.* at 14, 18-19, 21-22, 25-29.) Plaintiff's misrepresentation of Meyers's congressional testimony speaks volumes about the credibility of plaintiff's allegations overall. But because the Software and Testing Statements say nothing about CrowdStrike's Rapid Response Content testing and updating processes, plaintiff's allegations regarding the July 19 incident cannot prove that any of these statements were false. And even setting that threshold problem aside, the Software and Testing Statements are not actionable for several independent reasons.

First, plaintiff alleges that Sentonas made a false statement during an April 4, 2023 investor briefing—more than a year before the July 19 incident—when he said that CrowdStrike's "agent cloud architecture ensures that every agent is always up to date with the latest protection [and] doesn't require a massive tuning burden and doesn't blue screen endpoints with failed updates." (¶122 (citing Ex. R, at 6).) Plaintiff alleges that this statement was "false or, at a minimum, misleading *when made*" because CrowdStrike concealed that it was putting customers at risk of suffering blue screen outages. (¶123 (emphasis added).) But plaintiff takes this statement out of context. Sentonas's statement does not purport to guarantee that CrowdStrike would *never* cause a blue screen outage—and plaintiff fails to plead any particularized facts showing that the challenged statement was false *when made*, because the Complaint does not allege that the Falcon platform had caused any endpoints to blue screen with failed updates as of April 4, 2023. That a content update caused blue screen outages over a year after this statement does not adequately plead contemporaneous falsity of the challenged statement. *See Heck v. Orion Grp. Holdings, Inc.*, 468 F. Supp. 3d 828, 848 (S.D. Tex. 2020) (statement only actionable if "false when made").

Second, plaintiff targets a statement made in a CrowdStrike blog post published a year before the alleged Class Period, on November 17, 2021, that said "[f]or system stability, we always do canary deployments of new services before rolling out changes to the entire fleet." (¶139.) But the Complaint has not pled that this statement is false because it is does not (and cannot) allege that the July 19, 2024 content update was a "new service," as the Complaint does not identify a single instance of CrowdStrike ever suggesting that content updates are "services." *See Linenweber*, 693 F. Supp. 3d at 680 (rejecting falsity allegation where plaintiff misconstrued meaning of statement). Nor would a reasonable investor interpret "new services" to include Rapid Response Content updates, which the Complaint acknowledges are "regular, automatic updates" to the Falcon sensor. (¶¶22-23.) In fact, the blog post does not say one word about Rapid Response Content updates; instead, it is about "JSON Marshaling," which describes the process of converting data structures into a JavaScript Object Notation ("JSON") format. (*See generally* Ex.

S.) In context, this statement has absolutely no relation to plaintiff's factual allegations or the July 19 incident.

Third and fourth, plaintiff targets statements in CrowdStrike's 2023 and 2024 Annual Reports, that "[CrowdStrike's] technical staff monitors and tests our software on a regular basis," and that "[CrowdStrike] also maintain[s] a regular release process to update and enhance our existing solutions." (¶134 (citing Ex. C, at 16; Ex. T, at 15).) This allegation fails not only because the July 19 incident was not triggered by the release of a software update, but also because these statements are generalized statements that CrowdStrike "regular[ly]" tests and updates Falcon's software—*not* representations about specific features of the testing and updating processes used for Rapid Response Content updates or any other update, let alone guarantees of their effectiveness. *See Linenweber*, 693 F. Supp. 3d. at 678-79 (statement that company performed "regular maintenance checks" not false or misleading despite undetected issues because "regular" does not mean "exhaustive"); *Plains All Am.*, 307 F. Supp. 3d at 623-24 ("regularly asses[ed] pipeline integrity" not misleading despite issues with pipeline integrity because statement "was not about how well the [assessments] worked or that they were 100 percent effective"). Moreover, contrary to the allegation about a lack of regular testing and updates, plaintiff concedes that Falcon's software *did* receive "regular, automatic 'updates.'" (¶22.)[4]

Fifth, plaintiff alleges that Kurtz made a false or misleading statement at the 2022 Fal.Con conference when he declared that "[t]esting and validation is really important. We test more than anyone else, more than all of our next-gen competitors, more than other players that are out there."

[4] The statements above, about regular testing and updates—although entirely true—are also non-actionable because they are too generalized for reasonable investors to rely on. *See Van Ormer v. Aspen Tech., Inc.*, 145 F. Supp. 2d 101, 106-07, 107 n.5 (D. Mass. 2000) (statement that company could "enhance its software" was immaterial puffery).

(¶120.) Again, plaintiff strips this statement of its context and mischaracterizes it. The full transcript and accompanying presentation show that Kurtz was discussing *third-party* testing and validation of the Falcon platform's *efficacy* at preventing breaches, not for preventing crashes or bugs. (*See* Ex. U, at 5; Ex. V, at 10.) For example, Kurtz reported that the Falcon platform had achieved "100% protection" against malware after testing by AV-Comparatives, Mac Security Test and Review 2022. (Ex. U at 5; *see also* Ex. V, at 10.) Kurtz said nothing about CrowdStrike's *own* testing, and his focus was on third-party testing for *efficacy*—*i.e.*, how effective the Falcon platform is at stopping breaches—not on testing to ensure content or software updates do not trigger outages. Plaintiff ignores this context entirely and attempts to construe Kurtz's statement as describing CrowdStrike's *own* testing of its software updates, (¶121), but plaintiff's mischaracterization cannot give rise to securities fraud. *See Linenweber*, 693 F. Supp. 3d at 680. Moreover, plaintiff nowhere alleges that Kurtz did not consider testing or validation by third parties to be important, nor does plaintiff allege that CrowdStrike failed to submit the Falcon platform for third-party testing more often than its competitors. Absent such allegations, plaintiff fails to plead that this statement is false or misleading in context. In addition, Kurtz's statement is immaterial puffery. *See Ohio Pub. Emps. Ret. Sys. v. Meta Platforms, Inc.*, 2024 WL 4353049, at *5 (N.D. Cal. Sept. 30, 2024) (dismissing as puffery statement that "I think *we really do more than anyone else in the industry* on the safety and security front").

Plaintiff's only remaining factual allegations in support of its claim that the Software and Testing Statements were false or misleading are those attributed to three FEs—FE-1, FE-2, and FE-3—who all claim that, in their anecdotal experience, CrowdStrike was not testing its software in a pre-production environment or rolling out software updates in phases. (¶¶62, 63, 68.) Courts in the Fifth Circuit "*must* discount allegations from confidential sources," even at the motion-to-dismiss stage. *FirstCash Holdings*, 667 F. Supp. 3d at 306-07. FE-1, FE-2, and FE-3's allegations about software testing and updating should not be credited.[5] Plaintiff fails to adequately plead that these FEs were "in the position" at CrowdStrike where they would possess company-wide information about Falcon software testing and updating processes because none of them are alleged to have worked in a position at CrowdStrike that had anything to do with Falcon software testing or updating. *Izadjoo*, 237 F. Supp. 3d at 510 (FE must be described with "sufficient particularity to support the probability that a person in the position occupied by the source as described would possess the information pleaded"). FE-1 is the only FE of the three alleged to have had a job that involved testing, but as explained above, *see* pp. 11-12, *supra*, his position had nothing to do with content updates, coding, or software development or testing, and plaintiff does not allege otherwise. The same is true of FE-3, as also explained above, *see* pp. 12, *supra*. And likewise for FE-2, who allegedly worked in CrowdStrike's "IT department" and is not alleged to have had any involvement with content updates, coding, or software development or testing. (¶63 n.68.) Courts routinely reject FE allegations like these where the FEs purport to have knowledge about issues that do not relate to their specific job duties. *See, e.g.*, *Loc. 731 I.B. of T. Excavators & Pavers Pension Tr. Fund v. Diodes, Inc.*, 810 F.3d 951, 957 n.2 (5th Cir. 2016) (rejecting "anecdotal" FE allegations about matters "beyond their departments"). Also, FE-2's claim that "CrowdStrike's software update was not tested" should be discredited as conclusory, hindsight-based speculation, because it is nothing but his opinion that CrowdStrike "would have found the faulty update" had it conducted testing. *See KB Partners I, L.P. v. Pain Therapeutics, Inc.*, 2012 WL 12850252, at *9 (W.D. Tex. Sept. 26, 2012) (rejecting "conclusory" FE allegations).

[5] Plaintiff also cannot rely on allegations attributed to former employees quoted in the *Semafor* article, (¶75), which are not entitled to weight, *see* pp. 30-31, *infra*.

4. The Regulatory Compliance Statements Are Not Properly Alleged to be False.

Plaintiff is equally unsuccessful in alleging that CrowdStrike included two false statements on its website stating that CrowdStrike is approved by FedRAMP and DoD to do business with the federal government. (¶¶141, 143.)

Plaintiff fails to allege that CrowdStrike's statements that its products met the "stringent requirements" of the "FedRAMP program," and "Department of Defense Impact Level 4 (IL-4)," were false or misleading. (Ex. W, at 1; Ex. X, at 7.) The Court may take judicial notice of the fact that CrowdStrike's Falcon platform is listed on FedRAMP's marketplace as "FedRAMP Authorized," (Ex. D, at 68), and on the DoD Cyber Exchange as "Authorized," (Ex. E, at 1, 5). *Johnson v. Callanen*, 610 F. Supp. 3d 907, 910 n.3 (W.D. Tex. 2022). The Regulatory Compliance Statements merely reiterate what is stated by FedRAMP and DoD—FedRAMP and DoD both authorized CrowdStrike's Falcon platform. Because no allegation contradicts CrowdStrike's completion of FedRAMP and DoD authorization, plaintiff fails to allege that the Regulatory Compliance Statements are false or misleading. *See Plains All Am.*, 307 F. Supp. 3d at 621.

Because plaintiff cannot credibly allege CrowdStrike is *not* FedRAMP or DoD authorized, plaintiff tries to conjure falsity by pointing to the National Institute of Standards and Technology ("NIST") guidelines. Plaintiff's theory appears to be that FedRAMP and DoD require compliance with NIST Special Publication ("SP") 800-53 standards, including, allegedly, (a) testing software in a test environment, (b) conducting phased rollouts of software, and (c) maintaining a quality assurance team, which means that CrowdStrike's Regulatory Compliance Statements implicitly represent CrowdStrike followed those practices—even though CrowdStrike allegedly did not, which made the Regulatory Compliance Statements misleading. (*See* ¶142.)

This convoluted theory fails not only because it ignores that the incident was triggered by a Rapid Response Content update—not a software update—but also because the NIST provisions on which plaintiff relies simply do not require the specific testing, rollout, and quality assurance processes plaintiff claims. Plaintiff alleges that four NIST SP 800-53 standards in particular—known as AC-5, CM-2(6), CM-4(1), and SA-15—require staged testing, phased rollouts, and a quality assurance team. (*See* ¶¶37 & nn.22-23, 40 & nn.29-31.) Even a cursory review of those standards demonstrates that plaintiff has mischaracterized the standards.

As to CM-2(6), CM-4(1), and SA-15, plaintiff's allegations fail because these standards are *not required* for Moderate FedRAMP authorization or DoD Impact Level 4 authorization, which are the authorizations that plaintiff alleges CrowdStrike held on July 19, 2024. (*See* Ex. Y, at F-64 to F-66, F-68, F-174, F-177 (noting that products authorized at the Moderate level are not required to maintain a baseline environment for development and testing, analyze changes to the system in a test environment before implementation, or follow a documented development process).)[6] Therefore, the Regulatory Compliance Statements could never be construed as representing compliance with CM-2(6), CM-4(1), and SA-15. Plaintiff also mischaracterizes the remaining standard, AC-5. Plaintiff contends that AC-5 requires the maintenance of a quality assurance team for software testing; however, AC-5 merely requires that certain duties be performed by separate individuals or teams, and *as an example*, mentions separating "information system support functions" *such as* "quality assurance and testing." (*Id.* at F-18.) AC-5 plainly does not *require* that organizations maintain separate quality assurance and testing teams.

5. Plaintiff's Theory of Falsity Contradicts CrowdStrike's Disclosures and Is Impermissibly Based on Hindsight.

There are additional problems with plaintiff's theory of falsity, which cut across all of the categories of alleged misstatements. In particular, plaintiff ignores significant disclosures by

[6] CrowdStrike recently became FedRAMP High authorized. (Ex. Z, at 1-2.)

CrowdStrike that contradict key elements of plaintiff's theory, and plaintiff's own cited sources reveal that plaintiff's allegations are impermissibly based on hindsight above all else.

Plaintiff's allegation that CrowdStrike misled investors into believing CrowdStrike employed phased rollouts for Rapid Response Content updates is untenable, because that theory is contradicted by CrowdStrike's public disclosures. According to the Complaint, phased rollouts "requir[e] the 'gradual implementation of a new feature to a smaller cohort of users at one time rather than all users at once.'" (¶41.) No reasonable investor would have believed CrowdStrike followed that process for Rapid Response Content updates, because CrowdStrike has long disclosed that the Falcon platform was designed to identify threat activity and to automatically transmit security-related content updates "***in real time across*** [***CrowdStrike's***] ***global customer base.***" (Ex. C, at 4 (emphasis added); *see also* Ex. T, at 4 ("Falcon platform automates detection and prevention capabilities ***in real time across our entire global customer base***" (emphasis added).) As Sentonas explained, CrowdStrike ensures that "***every agent*** is ***always up to date*** with the latest protection." (Ex. R, at 6 (emphasis added).)

The suggestion that CrowdStrike led investors to believe that it rolled out content updates gradually, to "smaller cohort[s] of users" one at a time "rather than [to] all users at once," (¶41), is directly contradicted by CrowdStrike's disclosures that it "automates … prevention capabilities in real time across [its] entire global customer base," and keeps "every agent [] always up to date." (Ex. T, at 4; Ex. R, at 6.) Similarly, plaintiff implausibly alleges that CrowdStrike led investors to believe that each content update was rolled out in phases for "***24 to 48 hours***," (¶68 (emphasis added)), when CrowdStrike disclosed that content updates were transmitted in real time, to all customers simultaneously (*see* Ex. T, at 4; Ex C, at 5). CrowdStrike even explained that "real time" is akin to "seconds," not hours or days. (Ex. AA, at 5.)

Because CrowdStrike's actual disclosures do not support a claim of securities fraud, plaintiff alternatively alleges that every reasonable investor would have believed CrowdStrike tested Rapid Response Content updates in a pre-production environment, tested them with a separate quality assurance team, and rolled them out in phases, because allegedly "well-established industry standards and federal government requirements" required CrowdStrike to adhere to those practices. (¶2; *see, e.g.*, ¶¶33-42.)

This theory fails as an initial matter because Rule 10b-5 "makes it unlawful to omit material facts in connection with buying or selling securities when that omission renders '*statements made*' misleading." *Macquarie Infrastructure Corp. v. Moab Partners, L.P.*, 601 U.S. 257, 259 (2024) (emphasis added). A company's "failure to disclose information" cannot support a claim of securities fraud "if the failure does not render any 'statements made' misleading," because "[p]ure omissions are not actionable under Rule 10b-5(b)." *Id.* at 260. Plaintiff therefore cannot allege that investors were misled because they made assumptions about CrowdStrike's operations based on "industry standards" or the like, which CrowdStrike supposedly failed to correct. On the contrary, there can be no securities fraud unless CrowdStrike *itself* made "statements" that misled investors—which, as set forth above, plaintiff has entirely failed to plead. *Id.* at 264.

Furthermore, the Complaint does not plausibly allege the existence of any "industry standards" capable of supporting plaintiff's theory of fraud. *E.g.*, *Tung v. Bristol-Myers Squibb Co.*, 2020 WL 5849220, at *7-8 (S.D.N.Y. Sept. 30, 2020) (where allegations rest on "existence of a purported industry standard understanding," failure to sufficiently plead existence of industry standard means failure to allege actionable misstatement). For example, with respect to plaintiff's allegation that investors would have expected CrowdStrike to test Rapid Response Content updates in a pre-production environment, plaintiff cites three sources: two articles that *post-date the July*

19 incident (¶34 nn.14 & 16), and one undated article (¶34 n.13). None of these articles say that testing in a pre-production environment was universally practiced by cybersecurity firms, much less that cybersecurity firms universally did so during the entire alleged Class Period, or for updates to configuration data for identifying threats, which would be akin to Rapid Response Content updates. And plaintiff's reliance on articles that post-date the outage vividly illustrates the hindsight-based nature of plaintiff's theory of falsity. Just because the July 19 incident prompted some industry observers to recommend testing software and content updates in a pre-production setting, that does not mean investors *previously* had any basis to think CrowdStrike tested Rapid Response Content updates in a pre-production setting—particularly when CrowdStrike never said that it did. *See Heck*, 468 F. Supp. 3d at 854 (rejecting "classic fraud-by-hindsight pleading").

Plaintiff's allegations about "industry standards" for quality assurance are even more implausible. These allegations rely on a 2018 article about *the financial technology industry* that makes only a single passing reference to "quality assurance teams," (¶38 n.24), and two blog posts from *three months after the outage* that provide vague, high-level advice on how software companies can build effective quality assurance teams (¶38 n.25, ¶39 n.27). None of these sources remotely supports the allegation that every investor during the Class Period would have expected CrowdStrike to employ the specific kind of quality assurance team described in the Complaint—particularly in the absence of any representation from CrowdStrike to that effect.

With respect to phased rollouts, plaintiff again relies on four articles that post-date the July 19 incident, (¶41 nn.33, 35-37), and one 2021 blog post that said "many [companies] are *unable* to achieve successful phased rollouts at scale" (¶41 n.32 (emphasis added)). Setting aside that CrowdStrike's disclosures foreclosed the idea that Rapid Response Content updates were rolled out in phases, nothing in the Complaint plausibly alleges that "industry standards" would have led every investor to expect phased rollouts for Rapid Response Content updates during the alleged Class Period. And once again, plaintiff's reliance on post-outage news articles to support its allegations only underscores the impermissible, hindsight-based nature of the pleadings.

B. Plaintiff Fails to Plead Scienter.

Plaintiff's claim also fails because the Complaint does not adequately plead scienter. The Court can dismiss on this basis alone. *See Jastrow*, 789 F.3d at 534, 546-47.

Plaintiff must allege particularized facts giving rise to a "strong inference" that Defendants made the alleged misstatements (1) with an "intent to deceive, manipulate, [or] defraud"; or (2) were severely reckless. *Id.* at 535. Severe recklessness is "limited to those highly unreasonable omissions or misrepresentations that involve not merely simple or even inexcusable negligence, but an extreme departure from the standards of ordinary care." *Alaska Elec. Pension Fund v. Flotek Indus., Inc.*, 915 F.3d 975, 981 (5th Cir. 2019). This is a very high bar: a scienter inference must be "at least as compelling as any opposing inference one could draw from the facts alleged." *Tellabs Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 324 (2007). When the defendant is a corporation, courts determine scienter by "look[ing] to the state of mind of the individual corporate official or officials who ma[de] or issue[d] the statement." *INSpire*, 365 F.3d at 366.

1. Plaintiff Fails to Allege a Theory of Motive, Raising its Scienter Burden.

The first question in the scienter analysis pertains to motive: why would Kurtz and Sentonas implement allegedly deficient testing and update procedures and then lie about it, when, according to plaintiff, everyone would have known that doing so would set CrowdStrike on a path to inevitable catastrophe? This question is the essential starting point because, to plausibly plead scienter, it is "critical" for a securities plaintiff to plead that the defendants had a motive to defraud investors. *Mun. Emps.' Ret. Sys. of Mich. v. Pier 1 Imports, Inc.*, 935 F.3d 424, 431 (5th Cir. 2019). Motive serves as an "analytical device for assessing the logical strength" of a plaintiff's scienter allegations. *R2 Invs. LDC v. Phillips*, 401 F.3d 638, 645 (5th Cir. 2005) (quoting *Nathenson v. Zonagen Inc.*, 267 F.3d 400, 411 (5th Cir. 2001)).

But here, the obvious, most compelling inference is that Defendants had no motive to commit fraud—and plaintiff does not allege otherwise. Plaintiff's only apparent motive allegation is that Defendants "promoted and enforced … 'speed'" at the "expense" of testing to "maximize short-term profits." (¶112; *see also* ¶¶1, 8, 60-61, 73, 76.) But courts in the Fifth Circuit have routinely held that allegations of motives common to any corporate executive, like maximizing profits, fail to support scienter. *E.g.*, *Plaisance v. Schiller*, 2019 WL 1205628, at *21 (S.D. Tex. Mar. 14, 2019); *In re Franklin Bank Corp. Sec. Litig.*, 782 F. Supp. 2d 364, 388 (S.D. Tex. 2011) ("[A]chieving fast growth and profitability are well-recognized corporate goals, and show neither an intent to deceive, manipulate, or defraud, nor severe recklessness."). Plaintiff's motive theory does not support a cogent inference of scienter, much less a strong or compelling one, because plaintiff does not allege that Defendants personally acted to enrich themselves, or profited or benefitted from their alleged fraud in any concrete or particular way. *See Abrams v. Baker Hughes Inc.*, 292 F.3d 424, 434 (5th Cir. 2002) (no motive "[a]bsent an allegation that the defendants profited from the inflated stock"). Courts routinely reject similar boilerplate allegations of motives "universal to all corporate executives such as the desire to maintain a high stock price." *Plaisance*, 2019 WL 1205628, at *21. Here, the lack of any motive allegations weighs strongly against scienter and leaves a hole in the Complaint that none of plaintiff's additional vague, circumstantial scienter allegations comes close to rectifying.

2. Plaintiff Fails to Allege That Defendants Knew or Recklessly Disregarded Information That Contradicted Their Statements.

When, as here, a plaintiff fails to allege a "clear motive" theory, then—even at the motion-to-dismiss stage—the "strength of [the] circumstantial evidence of scienter must be correspondingly greater" than the very high bar that ordinarily applies even when motive is well-pled (and, here, it is not). *Neiman v. Bulmahn*, 854 F.3d 741, 748 (5th Cir. 2017).

To plead scienter based on circumstantial allegations, plaintiff must allege "very specific" facts showing that a "specific individual knew a specific statement was false at the time it was made," and those facts must be "correspondingly greater" in light of plaintiff's failure to allege motive. *Key Energy*, 166 F. Supp. 3d at 867; *Bulmahn*, 854 F.3d at 748. Plaintiff alleges that Defendants knew or were severely reckless in not knowing about testing deficiencies because of (i) warnings from former employees (¶¶108-10), (ii) two previous "faulty updates" (¶111), (iii) alleged "admissions" by company executives (¶¶92, 116), and (iv) a litany of miscellaneous allegations (¶¶98-103, 105-06, 114-15). These allegations, individually or together, cannot carry plaintiff's burden.

a. <u>The So-Called Employee Warnings Do Not Support Scienter.</u>

Plaintiff alleges that FEs "warned Defendants" that CrowdStrike lacked "adequate testing and … quality assurance." (¶108.) These allegations fail for lack of specificity and reliability.

First, FE-5 alleges that he sent a "video message" to Kurtz and Sentonas warning them of "understaffing" and unspecified "critical issues." (¶74.) But the video message is not alleged to have warned Defendants of anything to do with *testing* or *quality assurance* of software or content updates—the purported subjects of the alleged misstatements—so it cannot support scienter. *See Jastrow*, 789 F.3d at 542-44 (no scienter where warning email from confidential witness did not warn of the *specific* issue defendant allegedly knew about). Nor does plaintiff allege that FE-5 had firsthand knowledge that Defendants viewed the video message, as necessary to plead scienter. *See In re Affirm Holdings, Inc. Sec. Litig.*, 2024 WL 3955453, at *11 (N.D. Cal. Aug. 26, 2024). Instead, FE-5 relies on hearsay to claim that Kurtz and Sentonas watched the video. (*See* ¶109 ("FE 5 was told that Defendants Kurtz and Sentonas saw the video.").) But FE allegations that rely on hearsay are unreliable and should not be credited. *See Schulze v. Hallmark Fin. Servs., Inc.*, 2021 WL 3190529, at *5 n.41 (N.D. Tex. July 28, 2021) (noting that "[w]hen confidential witness statements contain hearsay and a plaintiff relies on that hearsay, courts have been skeptical even at the pleading stage" and collecting cases). FE-5 also alleges that Kurtz and Sentonas "would have known" CrowdStrike "lacked a dedicated quality assurance team." (¶109.) Such speculative "would have known" allegations also fail to support scienter. *Glaser v. The9, Ltd.*, 772 F. Supp. 2d 573, 594-95 (S.D.N.Y. 2011).

Second, plaintiff relies on allegations in an article published by *Semafor* that are imputed to anonymous former employees who are not identified as FEs. (¶¶75, 110.) These allegations fail because plaintiff does not even attempt to plead facts establishing the indicia of reliability that must be established before anonymous witnesses can be credited under the PSLRA. *See Izadjoo*, 237 F. Supp. 3d at 510. The *Semafor* article discloses the names of three of the former employees, two of whom—Jeff Gardner and Preston Sego—criticized CrowdStrike's quality control. (*See* Ex. BB, at 2-3.) However, Gardner was laid off and Sego was fired by CrowdStrike, both in 2023, well before the July 19, 2024 outage, and neither alleges that Kurtz or Sentonas *knew* of any testing or quality control issues, which is unsurprising given that neither was in a position to have firsthand knowledge of Kurtz and Sentonas's states of mind at the time of the alleged misstatements. (*Id.*) Gardner and Sego's reported accounts are also squarely contradicted by the third former employee named in the article—Joey Victorino—who described CrowdStrike as "meticulous." (*Id.* at 2); *see Applestein v. Medivation, Inc.*, 861 F. Supp. 2d 1030, 1038 (N.D. Cal. 2012) (rejecting allegations of one employee witness when contradicted by another). In any event, even if some unspecified "higher ups" and "company leaders" were allegedly warned of unspecified "issues" in unspecified "meetings, [] emails, and [] exit interviews," the allegations fail to establish that Kurtz and Sentonas themselves knew of any "issues" that contradicted their public statements when made. (¶¶75, 110); *see also Izadjoo*, 237 F. Supp. 3d at 517 (rejecting scienter allegation where confidential witness "[did] not state that he reported to the defendant [] officers, that they received the written reports, or that they knew the content of the reports"); *Flaherty & Crumrine Preferred Income Fund, Inc. v. TXU Corp.*, 565 F.3d 200, 208 (5th Cir. 2009). And the *Semafor* article is hearsay, which entitles it to even less weight. *See Schulze*, 2021 WL 3190529, at *5. The *Semafor* article accordingly does not support an inference of scienter.

b. <u>The Two Prior "Faulty" Linux Updates Do Not Support Scienter.</u>

Plaintiff also alleges that two allegedly "faulty updates" that affected Linux users on April 19, 2024, and May 13, 2024, support an inference of scienter. (¶111.) Not so. Plaintiff does not allege that Kurtz or Sentonas themselves knew about these updates. (*Id.*); *see TXU*, 565 F.3d at 208. In any event, plaintiff fails to plead any particularized facts about the two Linux updates, such as what caused the errors, whether it was the same cause as the July 19 incident, or even whether they involved software or content updates. *Dell*, 591 F. Supp. 2d at 894 (no scienter where allegations "lack specificity about what [defendants] knew or were reckless not to have known").

c. <u>Defendants So-Called "Admissions" Do Not Support Scienter.</u>

Plaintiff claims that Defendants' post-outage statements that "we got this wrong" and "we failed you," and the post-outage reports, support scienter because they were supposedly admissions that Defendants committed fraud. (¶¶92, 116.) These statements are not "admissions" of scienter because Defendants did not "admit[] that any of the alleged misrepresentations were false or misleading when made." *Heck*, 468 F. Supp. 3d at 854; *In re AppHarvest Sec. Litig.,* 684 F. Supp. 3d 201, 246 (S.D.N.Y. 2023). CrowdStrike's explanation that an error escaped multiple layers of testing and validation, (Ex. A, at 2), does not admit that any of its prior statements were false, let alone that Kurtz or Sentonas knew they were false. *See Heck*, 468 F. Supp. 3d at 854. Nor can plaintiff support its scienter allegations by noting that CrowdStrike implemented new testing procedures for content updates following the outage. (¶¶91-92); *Fener v. Belo Corp.*, 425 F. Supp. 2d 788, 815-16 (N.D. Tex. 2006) (rejecting argument that "corrective measures" contributed to inference of scienter). Plaintiff's admissions theory is "classic fraud-by-hindsight pleading that is not sufficient to raise a strong inference of scienter." *Heck*, 468 F. Supp. 3d at 854.

d. Plaintiff's Miscellaneous Scienter Allegations Fail.

Plaintiff offers a grab-bag of other allegations that amount to nothing more than insufficient speculation that Kurtz and Sentonas must have known their statements were false.

First, plaintiff claims that it was "obvious and known … to anyone at the Company" that CrowdStrike lacked a "quality assurance team … trained and equipped to assist with testing," and therefore Defendants acted with scienter. (¶105.) But as discussed at length above, CrowdStrike told investors it had a quality assurance team for testing for *accessibility*, which plaintiff does not allege was false. Nor does plaintiff allege how the lack of a quality assurance team for accessibility testing would have been "obvious and known" to Kurtz and Sentonas. Courts routinely reject allegations like these. *See, e.g.*, *Flotek*, 915 F.3d at 984.

Second, plaintiff alleges that Sentonas's "role and responsibilities" at CrowdStrike "strengthens the scienter inference." (¶115.) But courts in this Circuit regularly reject allegations that a defendant's position in the company contributes to a scienter inference. *See, e.g.*, *Shaw*, 537 F.3d at 535; *Izadjoo*, 237 F. Supp. 3d at 509; *Plains All Am.*, 307 F. Supp. 3d at 595.

Third, plaintiff claims that Kurtz and Sentonas must have known about alleged testing deficiencies because Falcon is CrowdStrike's "only product." (¶98.) Vague allegations of this type are routinely rejected under the PSLRA. *See, e.g.*, *Rosenzweig v. Azurix Corp.*, 332 F.3d 854, 867-68 (5th Cir. 2003) (rejecting argument that "failure of [defendant's] core business" supports scienter); *Collmer v. U.S. Liquids, Inc.*, 268 F. Supp. 2d 718, 754 (S.D. Tex. 2001) (same). And the Falcon platform is not CrowdStrike's "only product," as the Falcon platform includes numerous discrete products that can be purchased separately.

Fourth, plaintiff's allegation that FedRAMP "sworn declarations" contribute to scienter fails. (¶106.) Plaintiff fails to adequately allege that either Kurtz or Sentonas even signed such declarations, offering only the speculation of FE-8 that Kurtz, Sentonas, "or someone else in CrowdStrike's C-Suite" signed them. (¶107.) In any event, even if a declaration signed by an executive turns out to be false, that does not contribute to scienter unless there are "particular facts alleged to show that [defendants] knew that what they were certifying was not true." *Key Energy*, 166 F. Supp. 3d at 866; *Heck*, 468 F. Supp. 3d at 855. Plaintiff alleges no such facts.

Fifth, plaintiff alleges that CrowdStrike did not adhere to industry standards for software testing. (¶103.) As noted above, the incident was triggered by a content update, not a software update. But even setting aside that plaintiff has not plausibly alleged any relevant industry standards, courts in this Circuit have rejected these kinds of allegations because they say nothing about a defendant's *intent* with respect to alleged nonconformance with industry standards. *See, e.g.*, *Coates v. Heartland Wireless Commc'ns, Inc.*, 55 F. Supp. 2d 628, 636 (N.D. Tex. 1999).

Finally, plaintiff alleges that scienter can somehow be inferred because Defendants knew the general importance of testing and the risks of inadequate testing, as shown by (i) Defendants' emphasis on the importance of testing in public statements, including a book about cybersecurity, (¶¶99, 100, 114), and (ii) their experience working at another cybersecurity company, McAfee, when its product had an outage (¶¶101-02). Merely pleading knowledge of the *risk* of an outage due to alleged inadequate testing does not raise any inference that Defendants knew or should have known that allegedly inadequate testing was occurring at CrowdStrike or that any alleged statement was false. *See Pier 1 Imports*, 935 F.3d at 432. That is for obvious reasons: the argument that scienter can be inferred from knowledge of a risk would turn the law of risk warnings on its head and make it so that scienter could be successfully pled anytime a warned-of risk materializes. But the law is the opposite: when companies disclose a risk, it weighs against scienter. *Jastrow*, 789 F.3d at 540 (disclosure of "red flags" negates scienter).[7]

3. Plaintiff Cannot Plead Scienter as to CrowdStrike's Website Statements.

Plaintiff cannot plead scienter as to the four alleged misstatements published on CrowdStrike's website (¶¶139, 141, 143, 145), because plaintiff fails to plead particularized facts showing that Kurtz and Sentonas made, approved, or were even aware of these statements. To plead scienter as to unattributed statements or statements made by low-level employees, plaintiff "must first tie the statement to a corporate officer who can be seen as acting on behalf of the corporation in making the statement." *Plains All Am.*, 307 F. Supp. 3d at 627. Plaintiff relies on FE-8, who claims Kurtz and Sentonas "specifically directed" that "certain information" be put on the Company's website during an "all-hands meeting[]." (¶138 n.179.) But FE-8's allegation fails for lack of specificity: it does not allege that the "certain information" Kurtz and Sentonas directed employees to publish on CrowdStrike's website had anything to do with testing, let alone the specific website statements alleged to be false. And it is inherently implausible to think that either Kurtz or Sentonas dictated specific phrases for inclusion on the CrowdStrike website during an all-hands meeting. Plaintiff also alleges without any support that Kurtz and Sentonas "directed investors to read" CrowdStrike's website, (¶138), but that allegation is insufficient to tie these statements to Kurtz and Sentonas. *See Plains All Am.*, 307 F. Supp. 3d at 628.

[7] Plaintiff also resorts to group pleading by lumping Sentonas in with allegations that do not involve him. Contrary to plaintiff's claims, Sentonas did not "repeatedly tout" CrowdStrike's software updates. In fact, the Complaint includes only two quotes from Sentonas; neither discusses software updates. (¶¶100, 122.) Plaintiff's attempt to tag Sentonas with these allegations is improper group pleading that cannot establish scienter as to Sentonas. *See Shaw*, 537 F.3d at 533.

4. The More Plausible Inference Is That Defendants Thought Their Testing of Rapid Response Content Was Sufficient.

Plaintiff's scienter allegations are incoherent, and do not come close to being "at least as compelling" as the opposing non-fraudulent inference, as is necessary to avoid dismissal. *Jastrow*, 789 F.3d at 536. According to plaintiff, Kurtz and Sentonas were knowingly and deliberately setting CrowdStrike down a path to inevitable disaster by disregarding testing procedures that they allegedly knew were necessary to avoid incidents like that which occurred on July 19. Even more implausibly, plaintiff alleges that Kurtz and Sentonas embarked on this path to self-destruction without any motive to do so. These allegations fail to raise a plausible inference of scienter, let alone a strong one. *See Izadjoo*, 237 F. Supp. 3d at 518 (dismissing complaint where there was "little support for a plausible—much less strong—[scienter] inference.").

The much more compelling inference is that Kurtz and Sentonas believed that CrowdStrike's testing of content updates was sufficient and that additional or different testing was not justified given that content updates are not software or code and must be released frequently to address new threats. *See Jastrow*, 789 F.3d at 545-47 (affirming dismissal for lack of scienter and finding the more plausible inference was non-fraudulent); *Pier 1 Imports*, 935 F.3d at 434-37 (same). Because plaintiff has failed to allege an inference of scienter at least as compelling as any opposing inference, plaintiff's Complaint should be dismissed.

II. PLAINTIFF'S SECTION 20(A) CLAIM SHOULD BE DISMISSED.

Because plaintiff fails to state a claim for a primary violation of Section 10(b), its Section 20(a) claim automatically fails as well. *E.g.*, *Flotek*, 915 F.3d at 986.

CONCLUSION

The Complaint should be dismissed with prejudice.

Dated: April 7, 2025

Respectfully submitted,

/s/ Sandra C. Goldstein
Sandra C. Goldstein, P.C. (*pro hac vice*)
Kevin M. Neylan, Jr. (*pro hac vice*)
KIRKLAND & ELLIS LLP
601 Lexington Avenue
New York, NY 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900
Email: sandra.goldstein@kirkland.com
kevin.neylan@kirkland.com

and

Steven J. Wingard (State Bar No. 00788694)
Santosh Aravind (State Bar No. 24095052)
Robert “Robby” Earle (State Bar No. 24124566)
SCOTT DOUGLASS & McCONNICO LLP
303 Colorado Street, Suite 2400
Austin, TX 78701
Telephone: (512) 495-6300
Facsimile: (512) 495-6399
Email: swingard@scottdoug.com
saravind@scottdoug.com
rearle@scottdoug.com

Counsel for Defendants

CERTIFICATE OF SERVICE

I hereby certify that on April 7, 2025, a true and correct copy of the foregoing document was served via the Court's electronic CM/ECF filing system, which will send an electronic notification of such filing to all counsel of record.

/s/ Sandra C. Goldstein
Sandra C. Goldstein, P.C.